

portion of a nation-state's GDP all contribute to the problem, and are all being exploited by spammers.

2. A long list of laws prohibits spam. Perhaps the most elegant is the centuries old common law of trespass to chattels, which one judge in this District suggested fit the spam problem like a hand in glove. Notwithstanding that suggestion, a flurry of state and federal statutes have been passed over the last decade in an attempt to stop spam (or at least slow its growth) without unduly burdening "ham" (legitimate email). The culmination of this legislative activity was the Federal CAN-SPAM Act of 2003 (15 U.S.C. § 7701 et seq.).

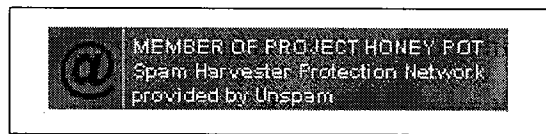
3. CAN-SPAM, it was hoped, would help stop spam by clarifying the rules that bulk emailers were supposed to follow. The reality is that legitimate emailers generally complied with CAN-SPAM long before it was enacted, or at least complied to the degree that the identity of someone who accepted responsibility for the mailing could be found on the face of the message itself. Spam is different. On its face, spam never identifies anyone willing to accept responsibility for the mailing. The reason is simple – spam violates the most basic standards of good conduct. Once identified, spammers cannot defend their "business" practices to anyone, let alone to an upstream webhost, email service provider or judicial fact finder.

4. If there were ever any doubt, today it is clear that the key to stopping spam is identifying those responsible for it, and getting that information into the hands of those willing and able to do something about it.

5. Discovering a spammer's identity is not simple, but it is not impossible either. To hide successfully, spammers have to do more than just avoid putting their name in their messages. Spammers must act anonymously, while simultaneously fooling their victims

(and everyone else who is providing them with some service essential to their criminal enterprise) into thinking they are running a legitimate business.

6. The first thing a spammer needs is a long list of email addresses to spam. Spammers get victim email addresses in two primary ways. They steal them (via harvesting from websites that display email addresses) or they guess them (via dictionary attacks). The most common way spammers steal email addresses is by harvesting them from websites, using web spiders. This makes life difficult for the rest of us because posting email addresses on a website is a convenient way to facilitate communications between visitors to a website and the owners of the website. Owners of websites who want to display email addresses can obtain some protection from harvesters by installing a honey pot from Project Honey Pot on their website, and displaying this Project Honey Pot logo on their website:¹



The logo serves as a warning to harvesters that all of the email addresses displayed anywhere on the website are protected by Project Honey Pot and deters harvesters by putting them at legal risk if they spam any addresses harvested from the website. Lawsuits of this kind are another effective way of deterring harvesters and the spammers who buy their harvested email lists.

7. Domain name owners who want to protect their email system from spam can obtain some protection by donating an MX record to Project Honey Pot, and then publicly disclosing the fact of their donation (but they should not disclose the specific MX record

¹ The website for the logo can be found at http://www.projecthoneypot.org/how_to_avoid_spambots_5.php.

donated, as spammers will simply avoid this MX record and continue to send spam to MX records not donated to PHP). By publicly disclosing their affiliation with Project Honey Pot, PHP members warn spammers that their domain names are protected by Project Honey Pot.

Project Honey Pot, a dba of Unspam Technologies, Inc.

8. Project Honey Pot (www.projecthoneypot.org) is a distributed network of spam-tracking honey pots. The Project allows spammers, phishers, and other e-criminals to be tracked throughout their entire "spam life cycle." On information and belief, Project Honey Pot was the first distributed e-mail harvesting research effort linking those that gather e-mail addresses by scraping websites with those that send unsolicited and frequently fraudulent messages. Tens of thousands of users from at least 100 countries actively participate in Project Honey Pot's effort to track criminals who break the law via email. Project Honey Pot was created by Unspam Technologies, Inc (www.unspam.com) – an anti-spam company with the singular mission of helping design and enforce effective anti-spam laws. Unspam Technologies, Inc. is a Delaware corporation with its principal place of business at 5278 Pinemont Drive Suite A-135, Murray, Utah 84123.

9. Project Honey Pot receives MX record donations from the owners of Internet domain names. Through those donations, email messages addressed to any username hosted at a donated domain name are directed to email servers owned and maintained by Project Honey Pot, and those email messages are then processed by and stored by PHP on computer equipment, including computer equipment located in Arlington, Virginia. Project Honey Pot also makes available to Internet website owners email address honey pots that can be installed on their webpages. When a harvester visits those webpages looking for email addresses to steal, the harvester is handed a unique email address hosted within Project Honey Pot's distributed

network of donated MX records. The harvester's IP address, the date and time of the visit and other characteristics of the harvester are recorded by Project Honey Pot and maintained for analysis and tracking. When a spam message is received thereafter at the unique email address, Project Honey Pot can tie the spam message (and the spammer) to the harvester that was given that email address.

10. Project Honey Pot is currently monitoring over 54 million honey pot addresses for annoying spam and dangerous phishing messages. Since Project Honey Pot first began monitoring spam, John Doe spammers have transmitted well over 1 billion spam messages to tens of thousands of unique email addresses belonging to PHP members who have donated an MX record to, and are receiving anti-spam protection from, Project Honey Pot. All of these email addresses were illegally harvested by the spammer (or a co-conspirator) from a website hosting a PHP honey pot, or were the subject of dictionary spam attacks that indiscriminately targeted random usernames hosted within Internet domain names that have donated an MX record to, and are receiving anti-spam protection from, Project Honey Pot.

11. Since it started collecting data in 2004, Project Honey Pot has identified over 80 million spam servers, over 96 thousand harvesters, over 14 million dictionary attackers, and since April 2007, has identified over 348 thousand comment spam server IP addresses.

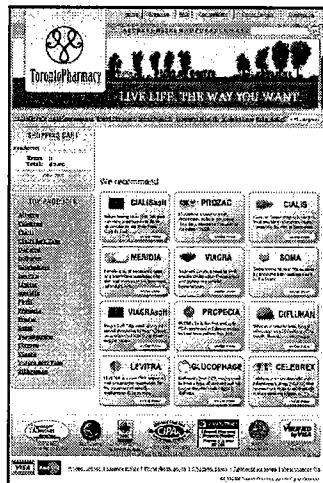
12. Every spam message transmitted to a Project Honey Pot honey pot email address harms Project Honey Pot. Each spam message is received by a mail server controlled by and paid for by Project Honey Pot, which then must process, store and analyze the message to help protect the website owners who have installed honey pots on their webpages from harvesters, and to protect the domain name owners who have donated MX records from spam attacks. Moreover, the spam received directly by Project Honey Pot is only a small fraction of

the total spam received by the domain name owners protected by Project Honey Pot. Project Honey Pot estimates that 125,000 spam messages are transmitted globally for every single spam message received by one of its honey pot email addresses. With over 1 billion spam messages in Project Honey Pot's inbox, this equates to 125 *trillion* spam messages transmitted globally since 2004 by all spammers, and roughly equates to hundreds of millions of spam messages transmitted globally by the Defendants in this case alone.

13. By this action, Plaintiff seeks against the Defendants: (i) an injunction to prevent further unlawful conduct; (ii) compensatory damages; (iii) punitive damages; (iv) attorneys' fees and costs of suit.

Defendants Andrey Chernuk and Boris Livshits, doing business as Toronto Pharmacy

14. On information and belief, Defendants Andrey Chernuk and Boris Livshits



are the owners of an illegal online pharmacy operating under the trade name "Toronto Pharmacy." Toronto Pharmacy operates through a host of domain names that all present a similar webpage layout and design to the viewer, as depicted here (a larger version is included as Exhibit A):

15. On information and belief, Toronto Pharmacy has used at least 170 different domain names to host its pharmacy business websites or to facilitate ancillary services necessary to its operations.

16. Between 2006 and the present, Toronto Pharmacy has been advertised in thousands of spam messages transmitted to email addresses managed by Project Honey Pot. Each of these spam emails advertised one or more of its websites, and each website could be visited by a viewer of the email by simply clicking on the link in the email message. A true and

correct copy of a sample of these spam messages is attached as Exhibit B. Some spam emails consisted of images of well-known brand name drugs with a hyperlink embedded in the image leading to a Toronto Pharmacy website. Other emails consisted of text and a hyperlink leading to a Toronto Pharmacy website. Sometimes the text in the email was arrayed in a multi-column table format. On information and belief, spam messages are arrayed across table columns to make it more difficult for spam filters to parse and thus block the message. On information and belief, each of the Toronto Pharmacy spam messages was transmitted to Project Honey Pot through a compromised “botnet” computer, and thus originated from an IP address fraudulently accessed by the Defendants, and each spam message contained a false or fraudulent email address in the from line.

17. Defendant Andrey Chernuk’s citizenship is unknown to Project Honey Pot. On information and belief, Mr. Chernuk has used at least two private mail box services in Florida to receive mail – one at 1901 60th Place E, Box L4385, Bradenton, FL 34203, and the other at 1455 Tallevast Road, Box L1128, Sarasota, FL 34243.

18. Defendant Boris Livshits’ citizenship is unknown to Project Honey Pot. On information and belief, Mr. Livshits was residing for a period of time relevant to this complaint at an apartment building in Brooklyn, New York. He has also used at least two private mail box services in Florida to receive mail – one at 2950 NE 32nd Avenue, Box A-1374, Fort Lauderdale, FL 33308-7219; and the other at 1903 60th Place E, Box M4283, Bradenton, FL 34203-5036.

19. In addition to operating Toronto Pharmacy, Defendants Livshits and Chernuk also operate other online businesses that may be advertised in other spam received by Project Honey Pot, including adult-content websites, computer software download websites, and

other pharmacy websites operating under different trade names. The full extent and nature of their related businesses are not yet known to Project Honey Pot.

JURISDICTION AND VENUE

20. This action arises out of Defendants' violation of the Federal CAN-SPAM Act. The Court has subject matter jurisdiction of this action based on 28 U.S.C. § 1331.

21. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or omissions giving rise to Plaintiff's claims, together with a substantial part of the property that is the subject of Plaintiff's claims, are situated in this judicial district. For example, 886 PHP members self-report they are located in Virginia. PHP members have installed honey pots on 287 websites that are hosted on IP addresses located in Virginia, and these Virginia-based honey pots have distributed tens of thousands of email addresses to identified harvesters world-wide. In addition, a substantial portion of the computer equipment used by PHP to process and analyze the spam messages is located in Arlington, Virginia. In addition to PHP's substantial presence in Virginia, the defendants also have substantial connections to Virginia. For example, Defendants have used compromised computers and/or IP addresses located in Virginia to transmit a portion of their spam messages. In addition, the webpages advertised in the spam messages were all visible in Virginia, and some of the prescription drugs advertised in the spam messages were shipped or delivered to physical addresses in Virginia.

22. The federal District Court for the Eastern District of Virginia has personal jurisdiction over Defendants based on the following facts: Defendants initiated emails from the Eastern District of Virginia, gained unauthorized access to computer servers located in the

Eastern District, caused tortious injury in the Eastern District, and conducted business in the Eastern District of Virginia.

COUNT I
Violation of the Federal CAN-SPAM Act (15 U.S.C. § 7701 et seq.)

23. Plaintiff repeats and re-alleges the allegations in paragraphs 1 through 22 of this Complaint.

24. Defendants initiated the transmission, to a protected computer, of a commercial electronic mail message that contained, or was accompanied by, header information that was materially false or materially misleading, in violation of 15 USC § 7704(a)(1).

25. In a pattern or practice, Defendants initiated the transmission to a protected computer of a commercial electronic mail message that did not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that a recipient could use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received, in violation of 15 USC § 7704(a)(3).

26. In a pattern or practice, Defendants initiated the transmission of a commercial electronic mail message to a protected computer and failed to provide: (i) clear and conspicuous identification that the message was an advertisement or solicitation; (ii) clear and conspicuous notice that the recipient could decline to receive further commercial electronic mail messages from the sender; and (iii) a valid physical postal address of the sender, in violation of 15 USC § 7704(a)(5).

27. Plaintiff is an Internet access service adversely affected by the above violations, and is entitled to an injunction barring further violations, statutory damages of \$100

for every attempted transmission of a spam message that contains false or misleading transmission information, statutory damages of \$25 for every attempted transmission of a spam message that otherwise fails to comply with the Federal CAN-SPAM Act, treble damages resulting from Defendants' use of email harvesters and dictionary attacks to facilitate their violations of the CAN-SPAM Act, and attorney fees and costs, as authorized by 15 USC § 7706(g).

COUNT II

Violation of Virginia's Anti-Spam Statute (18 Va. Code § 18.2-152.3:1 et seq.)

28. Plaintiff repeats and re-alleges the allegations in paragraphs 1 through 27 of this Complaint.

29. Defendants used a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers.

30. Defendants' transmissions were in contravention of the authority granted by or in violation of the policies set by Plaintiff. Defendants had knowledge of the authority or policies of those email service providers, or the authority or policies were available on Project Honey Pot's website.

31. As a result of Defendants' actions, Plaintiff has suffered injury, and is entitled to an injunction, and to recover actual damages, or in lieu thereof \$1 for each and every unsolicited bulk electronic mail message transmitted in violation of the statute, or \$25,000 per day any offending message was transmitted, plus attorneys' fees and costs of suit.

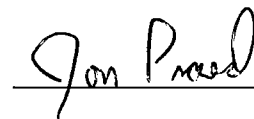
PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands this case be tried to a jury, and requests entry of judgment in its favor and against Defendants:

1. Granting preliminary and permanent injunctive relief against Defendants, and all those in privity or acting in concert with Defendants, enjoining them from directly or indirectly violating the terms of the CAN-SPAM Act or the terms of the Virginia anti-spam statute;
2. Awarding Plaintiff compensatory and punitive damages in an amount to be proven at trial;
3. Awarding Plaintiff attorneys' fees and costs associated with prosecuting this action; and
4. Granting Plaintiff such other or additional relief as this Court deems just and proper under the circumstances.

Dated: May 16, 2011

Respectfully submitted,



INTERNET LAW GROUP

Jon L. Praed (VSB #40678)
4121 Wilson Blvd, Suite 101
Arlington, Virginia 22203
(703) 243-8100 x223

*Attorneys for Plaintiff Project Honey Pot, a
dba of Unspam Technologies, Inc.*